

What is claimed is:

- 1 1. A method, comprising:
- 2 identifying a user using unique information;
- 3 designating a first plurality of files in a computer
- 4 as being associated with said user;
- 5 responsive to said identifying, using a program to
- 6 allow said user to make a change to any of said first
- 7 plurality of files associated with said user; and
- 8 preventing reading contents of said first plurality of
- 9 read/write files when said user is not identified.
- 1 2. A method as in claim 1, wherein said preventing
- 2 comprises encrypting said files using an encryption value
- 3 which requires said unique information to form an
- 4 encryption key.
- 1 3. A method as in claim 2, wherein said specified
- 2 information includes a user password.
- 1 4. A method as in claim 2, wherein said specified
- 2 information includes a unique number indicative of hardware
- 3 in the computer system.

- 1 5. A method as in claim 1, further comprising
- 2 designating a second plurality of files on the computer as
- 3 read only, and storing unencrypted information in said read
- 4 only files, but not allowing any changes to said read only
- 5 files.
- 1 6. A method as in claim 5, further comprising
- 2 establishing a plurality of special files within said
- 3 plurality of files, said special files being unencrypted
- 4 read/write files, and establishing special security
- 5 measures for said special files.
- 7. A method as in claim 6, wherein said security
- 2 measures include determining whether a specified program is
- 3 actually accessing the file, and only allowing file access
- 4 by said specified program.
- 1 8. A method as in claim 1, further comprising
- 2 detecting certain kinds of accesses based on specified
- 3 security criteria, and maintaining a log of said accesses
- 4 including information about a program that made said
- 5 accesses.

- 9. A method as in claim 1, wherein said preventing
- 2 comprises preventing certain users from obtaining access to
- 3 said files.
- 1 10. A method, comprising:
- 2 storing both encrypted and unencrypted files on a
- 3 computer;
- 4 starting an operating system by reading said
- 5 unencrypted files, and storing encrypted information
- 6 indicating results of computer operations.
- 1 11. A method as in claim 10, further comprising
- 2 designating unencrypted files as read only, and encrypted
- 3 files as read/write files.
- 1 12. A method as in claim 10, further comprising
- 2 forming encrypted files by requiring a unique information,
- 3 and using said unique as part of an encryption and/or
- 4 decryption operation.
- 1 13. A method as in claim 11, further comprising
- 2 establishing special files which are read/write files that
- 3 are not encrypted, and carrying out at least one security
- 4 measure on said special files.

- 1 14. A computer, comprising:
- 2 a processor;
- a file accessing element, controlled by a controlling
- 4 operation, said file accessing part controlling files in
- 5 the computer in a way that prevents access to specified
- 6 files but allows access to other files unless specific
- 7 unique information is used.
- 1 15. A computer as in claim 14, wherein said file
- 2 accessing element allows access to all read only files, and
- 3 prevents access to read/write files without said unique
- 4 information.
- 1 16. A computer as in claim 15, wherein said file
- 2 accessing element allows access to certain read write files
- 3 which are designated as being special, and also conducts a
- 4 security check before allowing said access to said read
- 5 write files.
- 1 17. A computer as in claim 14, wherein said file
- 2 accessing part controls said access by encrypting said
- 3 files.



- 1 18. A computer as in claim 17, wherein said
- 2 encrypting comprises obtaining personal information from a
- 3 user, and using said personal information to form
- 4 encryption and/or decryption operations.
- 1 19. A computer as in claim 18, wherein said personal
- 2 information is a password.
- 1 20. A computer as in claim 14, further comprising a
- 2 file storage part which includes removable memory, and
- 3 wherein unencrypted read/write access is allowed to said
- 4 removable memory.
- 1 21. A computer as in claim 14, wherein said file
- 2 accessing element is part of an operating system.
- 1 22. A method comprising:
- 2 identifying a user using unique information;
- 3 using an operating system associated program of a
- 4 computer to designate a first plurality of files in a
- 5 computer, as being associated with said user and to encrypt
- 6 said plurality of files using an encryption system that
- 7 includes said unique information;



- 8 responsive to said identifying, using said operating
- 9 system associated program in said computer to allow said
- 10 user to make any changes to any of said first plurality of
- 11 files using said encryption system associated with said
- 12 user and to prevent reading contents of said first
- 13 plurality of read/write files when said user is not
- 14 identified;
- 15 allowing other unencrypted files on said system to be
- 16 read when said user is not identified, but preventing
- 17 writing to said other unencrypted files; and
- 18 establishing special files on said system which are
- 19 unencrypted but which can be written to and read by the
- 20 system only after a specified security operation.
 - 1 23. A method, comprising:
 - 2 obtaining a unique code from a user of the computer
 - 3 system;
 - 4 determining specified files on the computer system
 - 5 which qualify for a specified security aspect; and
 - 6 encrypting all other files other then said specified
 - 7 files on said computer system, using said unique code.
 - 1 24. A method as in claim 23, wherein said unique code
 - 2 is a password.

- 1 25. A method as in claim 23, wherein said unique code
- 2 is a code from a smart card.
- 1 26. A method as in claim 23, wherein said unique code
- 2 is a code from a biometric.
- 1 27. A method as in claim 23, wherein said unique code
- 2 is a code from a digital certificate.